INTRUSION DETECTION USING FORENSICS AND PREVENTION FOR SECURE MANETS

# A PROJECT REPORT

*Submitted by*

**M. PREETHA MALINI**

**S. PRIYANKA**

**I. RUBINA BEGAM**

*In partial fulfillment for the award of the degree of*

**BACHELOR OF ENGINEERING**

*in*

ELECTRONICS AND COMMUNICATION ENGINEERING

# SSM INSTITUTE OF ENGINEERING AND TECHNOLOGY DINDIGUL-624002

**ANNA UNIVERSITY: CHENNAI-600025**

JUNE 2022

BONAFIDE CERTIFICATE

Certified that this project report “**Intrusion detection using forensics and prevention for secure MANETs”** is the bonafide work of “**M. PREETHA MALINI (922118106049), S. PRIYANKA (922118106052), I. RUBINA BEGAM**

**(922118106058)”** who carried out the project work under my supervision.

# SIGNATURE OF HOD SUPERVISOR

**Dr. S. KARTHIGAI LAKSHMI, Dr. K. VINOTH KUMAR**

**HEAD OF THE DEPARTMENT PROFESSOR**

Department of Electronics and Department of Electronics and

Communication Engineering, Communication Engineering,

SSM Institute of Engineering SSM Institute of Engineering

And Technology, And Technology,

Dindigul - 624002. Dindigul - 624002. Submitted for the VIVA-VOCE Examination held on

# INTERNAL EXAMINER EXTERNAL EXAMINER

**ACKNOWLEDGEMENT**

First and foremost, we would like to express our deep sense of gratitude to our most honorable Chairman and Management Trustee **Mr.K.Shanmugavel** of SSM Institute of Engineering and Technology for providing us with necessary facilities during the course of study.

We feel immensely pleased to express our sincere thanks to our Principal

**Dr.D.Senthil Kumaran** for encouragement and support.

We extend our solemn gratitude to **Dr.S.Karthigai Lakshmi**, Head of the Department, Electronics and Communication Engineering, for his timely support to all our activities. We express our sincere thanks to our guide **Dr.K.Vinoth Kumar Professor/ECE** for his guidance throughout our project work.

Also we express our thanks to the Faculty members of our Department, nonteaching staff members and my dear friends for their moral support, help and encouragement towards the successful completion of the project. We are most indebted to our parents, with whose support, resulted in making our dreams of becoming successful graduates, a reality.

# ABSTRACT

MANETS have become one of the most promising and interesting areas over the past few years. Security is one of the most important properties of MANETS, which are threatened by varied attacks, to approach practical deployment. Intrusion detection technology is a positive method to defense against security threats in MANETS. Construct a security ontology according to the features of MANETS to represent the formal semantics for intrusion detection. The ontology is used to improve the process intrusion detection for MANETS. propose an energy efficient routing method in an environment where both Attack detection and prevention schemes are used in MANETS. used to Intrusion Detection Efficient Routing Algorithm (IDER) For successful application of ubiquitous MANETS it is important to maintain the basic security. Which adopts the distributed architecture to monitor intrusion activities and realize abnormal events processing in local nodes. MANETS is a network with a large number of tiny sensor devices which are of low cost, and minimum consumption of power called as sensor nodes.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO** | **TITLE** | **PAGE NO** |
|  | ABSTRACT | IV |
|  | LIST OF TABLES | VII |
|  | LIST OF FIGURES | VII |
| **1** | **INTRODUCTION** | 1 |
| **1.1** | INTRODUCTION OF DIABETICS MELLITUS | 1 |
| **1.1.1** | DIABETIC RETINOPATHY | 1 |
| **1.1.2** | CAUSES OF DIABETIC RETINOPATHY | 1 |
| **1.1.3** | COMPLICATION OF DIABETIC RETINOPATHY | 2 |
| **1.2** | CLASSIFICATION |  |
| **1.2.1** | DEEP LEARNING | 3 |
| **1.3** | **METHODOLOGY** | 4 |
| **1.4** | **CONCLUSION** | 6 |
| **2** | **LITERATURE SURVEY** | 13 |
| **2.1** | EQUALIZING ENERGY  CONSUMPTION | 13 |
| **2.2** | DUPLICATE ADDRESS  DETECTION | 14 |
| **2.3** | POTENTIAL REPEATER NODE | 14 |
| **2.4** | TRANSMIT CONTROL AND DATA  SEPERATION | 15 |
| **2.5** | THROUGHPUT ENERGY  CONSUMPTION | 16 |

|  |  |  |
| --- | --- | --- |
| **2.6** | DETECTION FOR DATA  SECURITY | 17 |
| **2.7** | MONITORING COLLECTING AND  ANALYZE | 18 |
| **2.8** | EFFICIENT FOR LOCAL AND  GLOBAL LEVELS | 19 |
| **2.9** | MACHINE LEARNING TECHNIQUE  FOR INTRUSION | 20 |
| **2.10** | CONSTRUCTING A SECURITY RISK  FUNCTION | 21 |
| **3** | **SYSTEM STUDY** | 23 |
| **3.1** | **EXISTING SYSTEM** | 23 |
| **3.2** | BLOCK DIAGRAM OF PROPOSED  SYSTEM | 25 |
| **4** | **SYSTEM REQUIREMENTS** | 26 |
| **4.1** | HARDWARE REQUIREMENTS | 26 |
| **4.2** | SOFTWARE REQUIREMENTS | 26 |
| **4.3** | **FEASIBILITY STUDY** | 35 |
| **4.3.1** | TECHNOLGY AND SYSTEM  FEASIBILITY | 35 |
| **4.3.2** | ECONOMIC FEASIBILITY | 35 |
| **4.3.3** | COST BASED STUDY | 35 |
| **4.3.4** | TIME BASED STUDY | 35 |
| **4.3.5** | LEGAL FEASIBILITY | 36 |
| **4.3.6** | OPERATIONAL FEASIBILITY | 36 |
| **5** | **MODULE DISCRIPTION** | 37 |
| **5.1** | SOURCE NODE | 37 |
| **5.2** | ROUTING PATH | 37 |
| **5.3** | INTRUSION DETECTION  EFFICIANCY ALGORITM | 37 |
| **5.4** | SECURE COMMUNICATION | 38 |
| **5.5** | DESTINATION NODE | 38 |
| **6** | **SYSTEM TESTING** | 39 |
| **6.1** | TESTING PRINCIPLES | 39 |
| **6.2** | TEST CASES | 40 |
| **6.3** | SYSTEM IMPLEMENTATION | 41 |
| **6.4** | IMPLEMENTATION PLAN | 42 |
| **6.5** | EDUCATION AND USER  TRAINING | 43 |
| **7** | **CONCLUSION** | 44 |
| **8** | **FUTURE ENHANCEMENT** | 45 |

|  |  |
| --- | --- |
| **REFERENNCES** | 46 |

|  |  |  |
| --- | --- | --- |
| **CHAPTER** | **LIST OF TABLES** | **PAGE NO** |
| **3** | COMPARISION OF EXISTING LITERATURE | 23 |

|  |  |  |
| --- | --- | --- |
| **FIGURE NO** | **FIGURE NAME** | **PAGE NO** |
| **1.1** | CLUSTER INTRUSION | 3 |
| **1.2** | WARMHOLE ATTACK | 4 |
| **1.3** | DOS ATTACK | 7 |
| **3.1** | DETECTION EFFICIENT ROUTING  ALGORITHM | 25 |

**CHAPTER 1**

**INTRODUCTION**

The beauty of unsupervised method is that, it does not require any training data set or any kind of previous knowledge. An outlier is a behavior of data pattern which is significantly different from the remaining behavior of data. According to Hawkins definition the concept of an outlier is as follow s: “An outlier is an observation which deviates so much from the other observations as to arouse suspicions that it was generated by a different mechanism. Outlier detection techniques are becomes a very important technique in the field of computer security and data analysis.

# INFORMATION SECURITY

However, there are many security technologies like information security, unauthorized access prevention, and intrusion prevention, there are still many undetected intrusions. As an intrusion detection system to handle the enormous volume of information, it is also need to update the structure of an effective intrusion detection system is a complex and large project. Construction of the system staff relies heavily on the experience of their choice for the statistical anomaly detection means.

# Detecting Unknown Attacks

It can be a platform for the complete data acquisition, analysis and storage. Pedro Casasa. Which is capable of detecting unknown attacks over the network without using any kind of knowledge, traffic related data, or training data set. The authors use unsupervised approach for outlier detection that is based on Sub-Space Clustering and Multiple Evidence Accumulation techniques to point out the different kinds of network

intrusions and attacks, denial of services, activity of worms, unauthorized access to network resources, etc.

# Detection and Avoid Intrusion

Anomalous requests are processed by the Intrusion Detection System (IDS). The intrusion response component is the major responsible component in IDS for anomalous requests processing. Response component manages some of the policy for authenticating the user requests for further access. Recent necessity in the field of security and also the arguments among researchers are about designing a secure system which is proactive with appropriate security mechanisms. Most sensitive field of security that is emerging with its immediate needs is database security. Database security concerns the use of a broad range of information security controls to protect databases against compromises of their confidentiality, integrity and availability.

# CLUSTER BASED INTRUSION DETECTION SYSTEMS

People use the Internet for many purposes such as involvement in social media, currency transactions, exchange of personal information and also storing private data such as passwords, personal media, banking details like credit card credentials. The World Wide Web has advanced to such an extent that it has developed from a set of markup language sites to a place where performing remote actions on a network from anywhere in the world is an easy task. Surveys show that network intrusion crimes have increased drastically over the years and lead to personal privacy theft. The data that is stolen as part of personal privacy theft is sold in black markets. Hence there is a need to develop an effective and efficient network intrusion detection system for detecting the type of attacks.

The system uses clustering to detect the type of spams. Clustering is a type of unsupervised learning that involves the partitioning of a set of data into a set of meaningful sub-classes called as clusters. Most cluster-based intrusion detection systems use the traditional k-means algorithm to detect the type of attack.

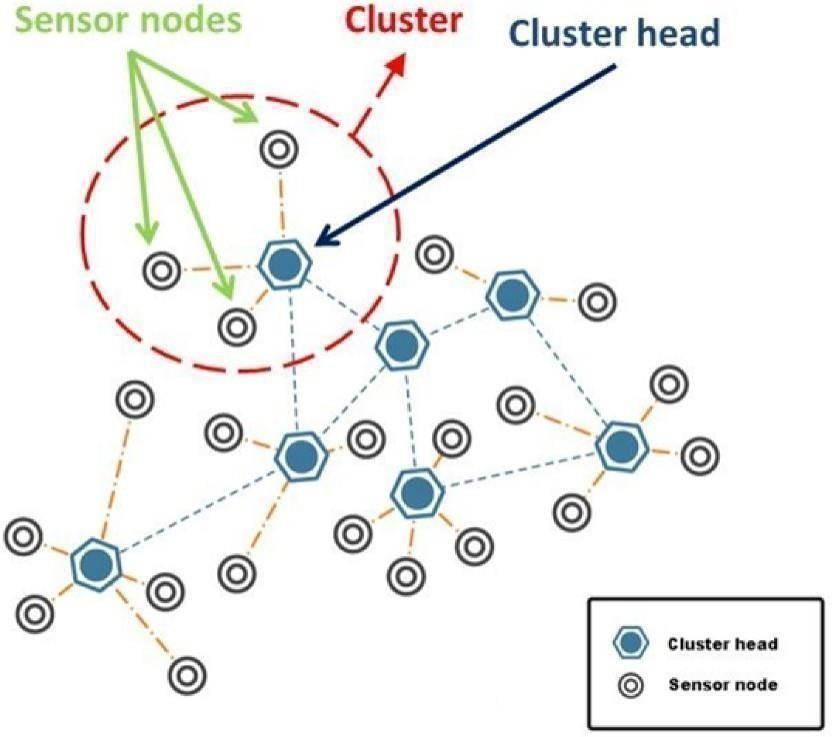


Fig 1.1 Cluster Intrusions

# Cluster

The Intrusion detection datasets are generally very large and contain many noncontributing features and redundant data. These drawbacks lead to inaccurate intrusion detection and increased computational cost when machine learning techniques are evaluated. Several data cleaning techniques have been proposed to eliminate redundant records and noncontributing features. These techniques reduce the size of the datasets significantly and make the characteristics of the data closer to the characteristics of intrusions in a real network. Support Vector Machine is a general learning algorithm derivates from statistics, it functions excellent in solving problems involved small sample, nonlinear, high dimension etc. advantages lies in its generalization ability, global optimization, having low sense with dimensions and its learning ability Current methods used for these systems include using anomaly detection or a signature database. Signature databases hold “definition s” of an

attack. A definition describes each attack that may occur in an environment. An anomaly is any unusual event that occurs in an environment. This method is used to detect attacks that have not been defined yet. The rule “anything that is broken in the house is considered an attack” will be a general anomaly that will be able to detect the definition previously provided.

# WARMHOLE ATTACK

Research we use both anomaly detection and a signature database using data mining techniques. Our solution provides a tool that would run data mining tools against a log file to detect patterns that may be considered an unauthorized activity. After the pattern is confirmed by the owner of the system as an attack, the attack pattern will be stored in a signature database. The tool gains additional patterns as time goes by and grows more effective. These organization’s only requirement is to protect their private and official data from the intruders and external, internal intruders. It may also be possible that some authorized user may leak the data.

organization for any purpose. In real-time, it is challenging to recognize the attacker because duplicate IP and attack packets can create.

Techniques used before like firewall, and IDS was not able to detect the real-time attackers which occurred in the absence of the admin without his knowledge. A computer network is the combination of a set of hardware and software.

Both components have their risks, vulnerabilities and security issues. The attack in the software makes the data vulnerable. The problem arrives when people don't have any underlying knowledge of programming, and their system gets attacked by the intruders, and they can’t find out the problem. The active attack is characterized by the attacker attempting to break into the system.

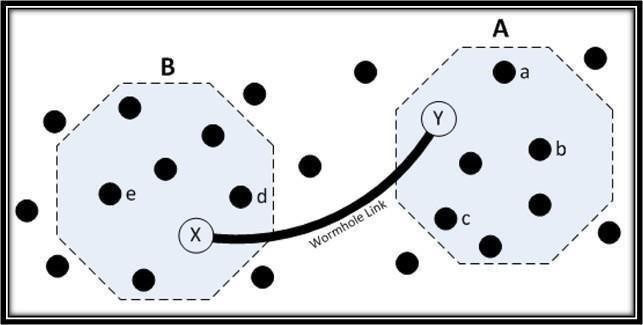


Fig 1.2 WARMHOLE ATTACK

According to the probability of packet delivery success of cluster topology is higher than that of star topology. In star topology, more end devices want to transmit its packet data, more collision happen due to several end devices sense channel idle in the same time and send packet in the same time. Besides that, end devices could not send its packet due to always sense channel in busy condition, thus it could not send its packet. The average delay in the cluster is not the same and not uniform, because the cluster topology depends on how many nodes and how many layers we split the node to be the end device and coordinator. It results the average delay data only slightly adrift. In the comparison of energy consumption, the need for energy consumption on a star topology is greater than the energy consumption on the cluster topology. It checks the data flow over the network in real time through hardware or software, and it compares it with the intrusion feature database in the system. Once it finds signs of being attacked, it immediately responds to the action defined by the user.

The underwater warfare is becoming the most important combat mode in future, therefore, development the underwater weapon and underwater communication

network is very important.

# STABLE WORKING ENVIRONMENT

Openness to the deployment area network s pose a huge security risk. Since node power energy, computing speed, storage space and communication capabilities are very limited, how to design effective security mechanism to ensure the network data security. prevention of various types of malicious attacks, enabling wireless sensor networks can be a safe and stable working environment, will affect the wireless sensor network technology can really go toward practical applications. Sensor networks is usually based on node location and external environment is divided into several clusters, each cluster nodes and the nodes in the cluster is divided into the ordinary nodes, at the same time so me common node is used as intrusion detection.

# Packet Transmission

The function of ordinary nodes is collecting data and to transmit data; Detection node is responsible for detecting whether the attack; Summary node detection node can be sent to the test results summary, judged by the summary is also exist in the network intrusion behavior. Determine the necessary nodes and redundant nodes in network, then will be deployed on the detection node detection algorithm. In order to improve the security of wireless network, an anomaly intrusion detection algorithm based on adaptive time-frequency feature decomposition analyzes the types and detection principles of wireless network intrusion detection.

# Statistical Analysis Method

How to actively defend and effectively suppress all kinds of illegal acts on the network? Itis an important problem to be solved in the field of computer network security., it adopts the information statistical analysis method to detect the network intrusion, constructs the traffic statistical analysis model of the network abnormal

intrusion, and establishes the network intrusion signal model by combining the signal fitting method With the opening of computer network technology and the expansion of the degree of sharing and interconnection, the security and reliability of the network has become a common concern of users at different levels of use.

# Denial of Service Attacks

It is generally believed that the security threats to computer network systems mainly come from three aspects: hacker attacks, computer viruses and denial of service attacks. There are numerous tools to perform DoS attack from millions of compromised system and can mess up any system or network in short period of time. There are many Weil known counter measures available like puzzle based defense mechanism. Denial of service attack is an attempt to make a machine or a network unavailable to its users, such as to temporarily or permanently interrupts its services. Vulnerabilities such as Hack bomb, stream multiplexing, protocol upgrades and invalid frame states are discussed in propose attack models based on invalid frame state, which exhausts server resources by continuously sending specific request packets to the server, causing the serve r to refuse service. A sample website was hosted in each server’s home directory. This website contains a homepage in which twenty- two images are embedded. We also designated another computer in the network as malicious client.

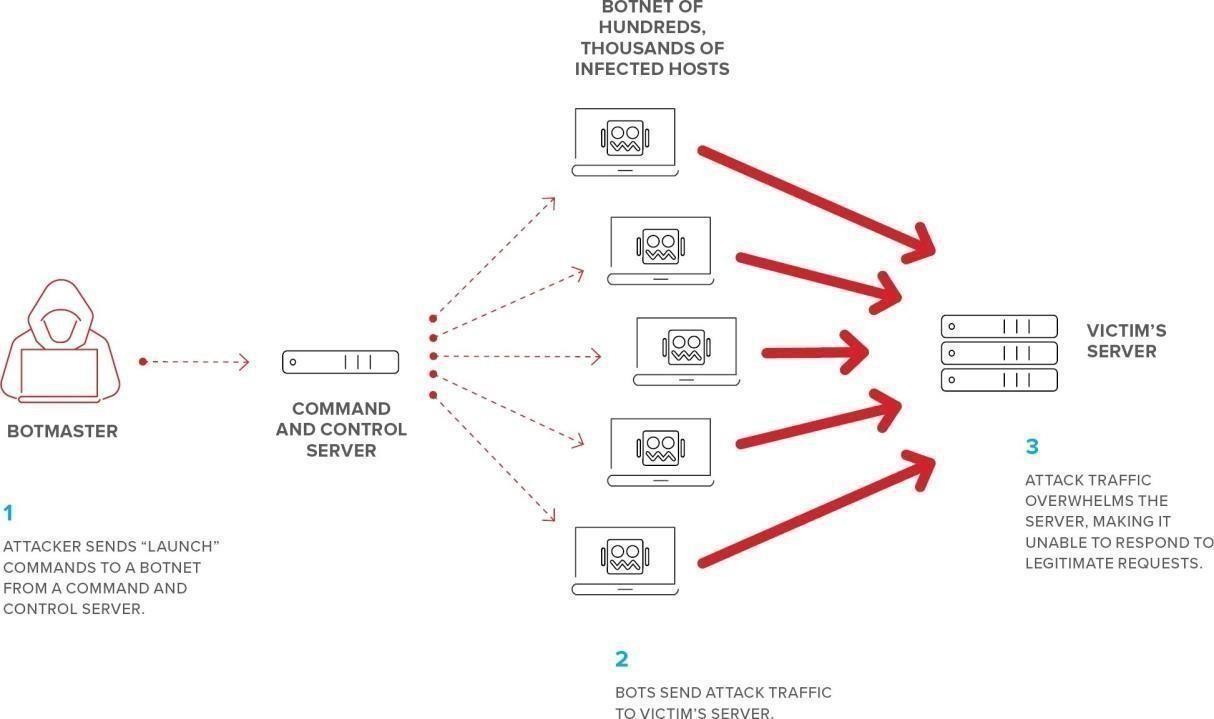


Fig 1.4 DOS Attack

For a long life of sensor node and a high spectrum efficiency of frequency spectrum, the sensor node uses the transmission control of event driven sensor.

As a result, the variation range of future sensing information is predicted. When some sensor send sensing information to the variation ranges of future sensing information maybe duplicated. It indicates that the difficulty of data separation by becomes high. The proposed method sends command to the specified sensor nodes to stop the event. Therefore, the highly accurate data separation is possible. In our proposed transmit control, the process of event driven is maintained while the can surely separate each sensing information. The redundant sending of sensing information. The detected sensing information can be separated for the several sensor node by data tracking based on the peculiar time continuity of sensing information.

# BENEFITS OF NETWORK SECURITY

**COST**

Networking eliminates the capital expense of buying hardware and software and setting up and running on-site datacenters the racks of servers, the round-the-clock electricity for power and cooling, the IT experts for the biggest Network services run on a worldwide network of secure datacenters, which are regularly upgraded to the latest generation of fast and efficient computing hardware. This offers several benefits over a single corporate datacenter, including reduced network latency for applications and greater economies of scale managing the infrastructure

# GLOBAL SCALE

The benefits of Network Transmission services include the ability to scale elastically. In cloud speak, that means delivering the right amount of IT resources

# SECURITY

Many cloud providers offer a broad set of policies, technologies and controls that strengthen your security posture overall, helping protect your data, apps and infrastructure from potential threats. The throughput and the delay of the network have been compared for these three scenarios. Having a network with l over delay is desired for increased efficiency.

# SPEED

Most intrusion detection services are provided self service and on demand, so even vast amounts of Networking resources can be provisioned in minutes, typically with just a few mouse clicks, giving businesses a lot of flexibility and taking the pressure off capacity planning..

# RELIABILITY

Network security makes data backup, disaster recovery and business continuity easier and less expensive because data can be mirrored at multiple redundant sites on the cloud provider’s network.

# SCALABILITY AND FLEXIBILITY

Network can assist companies to start with a small set up and grow to a large condition fairly rapidly, and then scale back if necessary. Also, the flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands. Moreover, cloud computing is ready to meet any peak time requirement by setting up with high capacity servers, storages etc.

# CHARACTERISTICS OF NETWORK ON-DEMAND SELF-SERVICE

On-demand self-service means provisioning or de-provisioning computing resources whenever required in an automatic fashion without human intervention. An analogy to cloud computing is electricity as a utility wherever a client can activate or deactivate a switch to use the electricity as needed.

# UBIQUITOUS NETWORK ACCESS

Ubiquitous network access means that computing facilities can be accessed from any place with any computing devices such as smart phones, tablets, laptops, personal computers and so on.

# RESOURCE POOLING

In resource pooling computing resources pooled to satisfy the demand of the

customers so that resources (physical or virtual) will dynamically be allotted, reassigned

order- allocated as per the need.

# MEASURED SERVICE

Measured service suggests that customers solely get the computing resources that they have paid. This idea is analogous to utilities like water or electricity.

# DISADVANTAGES OF INTRUSION DETECTION INTERNET CONNECTION

For cloud computing, an internet connection is must to access and appreciate cloud services.

# LOW BANDWIDTH

The advantages of cloud computing cannot be used by low bandwidth internet connection. Even a high bandwidth satellite connection will result in poor quality performance because of high latency.

# SECURITY ISSUES

Security is the major concern in cloud computing. The cloud consumer’s valuable and confidential data is stored and processed in the cloud through internet which is susceptible to attacks. If security management is not properly provisioned then the business and data will become prone to hackers and threats.

# NON-NEGOTIABLE AGREEMENTS

A few cloud computing providers have unnegotiable contracts for the businesses.

It may be negative for lots of companies.

# LACK OF SUPPORT

Network-based services do not always provide proper support to the customers. The vendors are not available on e-mail or phones and demand the consumers to

depend on FAQ and online community for support. Due to this, complete transparency is never offered.

# INCOMPATIBILITY

Sometimes, there are problems of software incompatibility. Some applications, tools and software are incompatible to connect to a particular personal computer.

# MINIMAL FLEXIBILITY

Because of the applications and services run on a remote server, the consumers using cloud computing have minimal control over the functions of thesoftware as well as hardware. The applications can never be run locally due to the remote software.

# CHAPTER 2 LITERATURE SURVEY

**EQUALIZING ENERGY CONSUMPTION**

Fei Geoetal., (2013) Wireless Sensor Network ( W S N) have emerged as an important area for research and development because of their application such as in e-healthcare monitoring system. Presents and discusses the performance of slotted and unslotted Carrier Sense Multiple Access with Collision Avoidance protocol WSN for medical system, with a few additions to the protocol and adequate tuning parameters. Increasing rapidly in size and complexity due to recent advances in radio frequency, computing, and sensing technology. This technology is used to allow applications utilize hundreds or thousands of sensor nodes. Application of WSN are used in various ways, for example at the military is used to make observations on the battlefield, or used to monitor the health state of a patient in a room.

Usually, WSNs node is powered by independent batteries.. Therefore, to reduce energy consuming and to prolong the lifetime of WSNs is still a critical issue in research. There are two main methods being adopted by researchers: one is equalizing energy consumption of nodes in network; another one is improving energy efficient of nodes. Thus the optimization for one layer cannot guarantee the entire network optimization. Our proposal ’s design thinking is: when a node wants to select a new route, it will choose those nodes whose residual energy is higher and the location is closer to destination node to be a relay node as its next hop. This scheme could avoid the disequilibrium of the node’s energy consumption and an overlong propagation route.

# DUPLICATE ADDRESS DETECTION

Hyung-Sinetal.,(2012) However, when applied to a large scale WSN, it may not provide desirable node connectivity mainly due to the waste of network depth and networking bias. we consider the design of network joining algorithms that can construct a large-scale cluster-tree structured WS N with maximal node connectivity.

A new node willing to join as a router selects its parent node among neighbor routers which are closer to the network coordinator than itself, reducing the waste of network depth. The parent node selects isolated nodes first as its child routers, alleviating the networking bias problem.

Finally, the performance of the proposed networking mechanism is verified by computer simulation, showing remarkable performance improvement over conventional Zig Bee in a large scale WSN.

To alleviate the networking problems occurred in conventional Zig Bee, we have design a new parent/child selection scheme for the construction of cluster-tree structured WSNs. New child nodes select their parent considering the network depth of neighbor routers, while the parent node selects its child routers considering the RSSI or the number of potential parents.

# POTENTIAL REPEATER NODE

A ChimBergeretal .,(2012). A major task of wireless sensor networks ( WS N s) is to collect data under a range of ambient conditions and with many different dynamics from a variety of sensors which are distributed, for instance, around an industrial plant. Focusing on real-time data collection for control applications, we present a spatial extension to our previously published self-organized TDMA-

based WSN with star topology implemented on low-complexity commercial off-the-

shelf hardware. Miniaturized, battery powered, self-sufficient sensor nodes are sensing physical properties and the wireless sensor network (WSN) is responsible for transmitting these data to a base station for further processing.

Depending on the application, constraints on data traffic can be diverse, prioritizing features such as real- time capability, reliability, scalability, deterministic behavior, and low power consumption. In this contribution, we restrict ourselves to WS Ns with a star topology and a main-powered base node. This is a reasonable assumption for many industrial applications, where access to fixed infrastructure .Finally the network should support self-configuring and dynamic joining and leaving of nodes.

Real-time behavior is achieved by assigning a fixed time slot in each beacon- triggered time- interval (super frames) to data transmission to each sensor node. This allows use of the sensor data not only for monitoring but also for control purposes.

# TRANSMIT CONTROL AND DATA SEPERATION

Kyosuke Fukudaetal., (2018) uses the frequency modulation of sensing information and recognizes the whole sensing information from the detected frequency spectrum. F or long life sensor node, the event driven sensor decides to send the sensing information in accordance with the certain amount of changing about the sensing information. However, the data separation is difficult for the PhyC-S N with event driven sensor. The transmit control and the data separation for PhyC- SN with event driven sensor. The Gaussian probability model for predicting the future sensing information is used for estimating the difficulty of data separation. The effect of proposed technique is evaluated by computer simulation. In FC, the existence of spectrum component from the received carrier signal can be detected by the spectrum analyzer of fast Fourier transform(F FT). Since the frequency of detected spectrum indicates the level of quantized sensing information, FC can recognize the quantized sensing information.

Although some sensors simultaneously access FC, FC can detect all the

quantized sensing information by FFT in one time. In addition, PhyC-S N can also separate each sensing information with data tracking based on the peculiar time continuity of sensing information. For long life of sensor node and high spectrum usage efficiency, the sensor node of event driven is considered. The sensor node does not send information until the sensing information is changed over the certain level. The transmit control and the data separation with using the prediction of sensing information. The linear function model based on the minimum mean square error (MMSE) criterion is derived from the memorized sensing information during certain duration. The future sensing information is predicted by the extrapolation of linear function. In addition, the fluctuation of past sensing information can be modeled by Gaussian PhyC-SN probability process. As a result, the variation range of future sensing information is predicted. When some sensor send sensing information to FC, the variation ranges of future sensing information.. The advances of micro sensor s, embedded, and wireless communication technologies have lead the emerging of wireless sensor network (WSN) which already conducted and tested in different application area, such as industrial and health application.

# THROUGHPUT, ENERGY CONSUMPTION

M. UdinHarun AlRasyidetal.,(2015)Performance of beacon enabled and non- beacon enabled were evaluated and analyzed to understand the impact of protocol parameters such as Super frame Order (SO), Beacon Order (BO), and Traffic Load. The performance of the network which have been evaluated in detail are the throughput, energy consumption, end to end delay, packet success probability, drop packets and the percentage of the energy efficiency. The simulation result show that of beacon enabled is better than non-beacon enabled in terms of the throughput, drop packet, energy consumption, and energy efficiency. However, there are two problems for constructing the data group in the Phy C-S N with TCED. First, the accuracy of estimating the time continuity of sensing

information becomes worse than that without TCED because some sensing

information are not sent.

Especially, when the amount of change in sensing information is small, the more sensing information are not sent. Therefore, two problems becomes more serious. If the separation of sensing information is error, the error is propagated to the other sensing information in a chain reaction by tracking.

The big drop packets that can be caused due to line quality is not good, packet duplication, busy MAC layer, routing fails, the MAC layer cannot transmit packets and the queue is full. While the drop packet of non-beacon enabled is higher than beacon enabled, because non beacon enabled using un slotted CSMA/CA and only needs one time CCA. When FC pays attention to memories, the difference between the past sensing information and the constructed linear function is evaluated and it is caused by the disturbance of various noises.

# DETECTION FOR DATA SECURITY

Manoj Kumar etal., 2014 the beauty of unsupervised method is that, it does not require any training data set or any kind of previous knowledge. Unsupervised outlier detection techniques are playing big role in various application domains such as network intrusion detection, fault detection and fraud detection. Basically, outlier represents that behavior of data which is different from the other expected behavior of data. And, outlier detection is a process of finding outliers from the last few decades, there has been a lot of research in this field. Outlier detection has different areas of application like intrusion detection for data security, network security, credit card fraud detection, insurance fraud, fault detection in real time safety critical systems and defiance activities. In recent years, cyber- attack and network security incidents show a rising trend. However there are many security technologies like information security, unauthorized access prevention, and intrusion prevention, we have presented can be implemented in real time environment also. Construction of the system staff relies heavily on the

experience of their choice for the statistical anomaly detection means. It can be

a platform for the complete data acquisition, analysis and storage.

But it still needs security expert analysis and classification of pre-attack means and weaknesses in the system and then manually prepared by the relevant rules and mode of misuse detection. The importance of outlier detection is due to the fact that outliers in data move to significant information in a different variety of application areas. Recently, the technique of outlier detection is continuously gaining attention.

# MONITORING COLLECTING AND ANALYSING PERFORMANCE

Ramdhani Ismaretal., (2015) variation of traffic load against the drop packet. Number of packet drop may indicate network performance, the smaller the drop packets that occur the better the performance of network. In the event of a drop packets on a network, the network throughput gets low. The big drop packets that can be caused due to line quality is not good, packet duplication, busy MAC layer, routing fails, the MAC layer cannot transmit packets and the queue is full. While the drop packet of non-beacon enabled is higher than beacon enabled, because non beacon enabled using un slotted CSM A/CA and only needs one time CCA. So the probability of transmitted packet is greater.

As Intrusion detection system to handle the log information of various machines and their service activities, it is also need to update the structure of an effective IDS is a complex and large projects because of large number of resources. With so many resources, it is not reasonable to monitor anomalies. To detect intrusions, first we need to collect log database of network. Abnormal activities are usually done by monitoring, collecting and analyzing performance counters. Proposed an un supervised modified means algorithm for identifying outliers. .They compare algorithm with existing algorithm and benchmark performance, they found more efficient result then oth implemented with different situations to evaluate whether identified outlier is bers. They also by chance or not. The identified outliers and

then removed from the data set to enhance clustering accuracy. According to

authors, most of Intrusion Detection Systems are used in real-time applications. IDS should be simpler but efficient enough to detect intrusions quickly. Distance- based Outlier Detection is a method for detecting outliers.

Although the authors used high-dimensional data-sets for IDS s, yet it is a dimensionality issue to use this approach. Proposed an un supervised modified means algorithm for identifying outliers. They also implemented with different situations to evaluate whether identified outlier is by chance or not. The identified outliers and then removed from the data set to enhance clustering accuracy. Pointed to real time analysis of intrusion detection problem and also suggested its solution. According to authors, most of Intrusion Detection Systems are used in real- time applications. IDS should be simpler but efficient enough to detect intrusions quickly.

# EFFICIENT FOR LOCAL AND GLOBAL LEVELS

Wael Ali Hussein et al.,(2017) they have been designed for scalar data such as sensor data; which is small in size compared to multimedia data.. The addressed challenges were the motivation to design mobile reliable routing protocol based on greedy routing structure. Although the authors used high- dimensional data-sets for IDSs, yet it is a dimensionality issue to use this approach. Proposed a clustering approach based anomaly detection method (CLAD) that is capable to detect suspicious pattern of data sets that are deviate much from nor m al data sets. To detect suspicious clusters, they populated the size of cluster and its location and behavior relative to other clusters. Presented an effective model ,called(Maximal Patterns for Intrusion Detection), that used maximal frequent patterns mining to detect intrusion and generate rules using inference that not need to define all association rules and patterns discovery. This algorithm is very novel and efficient for detecting intrusions from network data. After implementation of MID, results are very accurate and performance of algorithm is robust for those attacks that are unseen

or not active. It used tcp dump data file to check user’s log file from the network

activities.

The majority of activities are considered as nor m al. These activities those are frequently recurring and their behavior is normal. Attacking activities has different behavior than nor m a l activities.

These activities those are not frequently recurring, i.e. some activities occur for short period of time and not seen by network operator, treated as intrusion. So we follow the frequent patterns analysis with the labeled data set. Author explains the phases for detecting intrusion. First is training phase and second is testing phase. The World Wide Web has advanced to such an extent that it has developed from a set of markup language sites to a place where performing remote actions on a network from anywhere in the world is an easy task. Surveys show that network intrusion crimes have increased drastically over the years and lead to personal privacy theft.

# MACHINE LEARNING TECHNIQUES FOR INTRUSION

Wael Ali Hussein etal.,(2017).The conflicting of WMS N parameters are almost impossible to be solved in terms of physical nature of the hardware components, however, optimal balance

between energy consumptions and QoS can be achieved. The power consumption in sensor nodes result from two parts: radio transceiver and data computation and processing. The data that is stolen as part of personal privacy theft is sold in black markets. Hence there is a need to develop an effective and efficient network intrusion detection system for detecting the type of attacks. Intrusion detection datasets play a major role in evaluating machine learning techniques for Intrusion Detection Systems. The Intrusion detection datasets are generally very large and contain many noncontributing features and redundant data. These drawbacks lead to inaccurate intrusion detection and increased computational cost when machine learning techniques are

evaluated. Several data cleaning techniques have been proposed to eliminate

redundant records and noncontributing features. This paper identifies anomaly problems in norm al and intrusion attacks data.

Computer Communication Networks suffer from several security threats including intrusion attacks

To address this security problem, the intrusion dataset generated in a network are generally very large and the data (normal or attacks) are usually recorde d over very long period of time. Similarly the anomalies should not be misinterpreted as normal.

These changes in spatial patterns can be observed by applying the proposed pseudo- space, ellipsoid-based, data approximation technique iteratively and determine normal data. Conventional intrusion detection system used packet classification and deep packet inspection, which may not be sufficient to detect all kind of network intrusions, therefore, we are trying new approach for detecting attacks. And propose a new statistical waveform based for packet classification. Our attention is on statistical data of waveform features, and we use their feature extraction s as the input of the classifiers. In addition, a multi-classifier is proposed to make the final decision. Bayesian network, also called evidential network, is the expansion of the Bayesian method, and one of the most efficient model in uncertain knowledge and reasoning field. It can be used to express and analyze uncertainty and probability event, and conditionally rely on decision-making with a variety of control factors, make reasoning from uncompleted, imprecise or uncertain knowledge or information.

# CONSTRUCTING A SECURITY FUNCTION

Haihui Geet al., (2010) to evaluate the security situation of hierarchical network, a novel evaluation algorithm based on the method of constructing a security risk function is proposed. The proposed algorithm is the aggregation of qualitative evaluation and quantitative evaluation. Many mathematical algorithms

have been applied in the field of network security evaluation. The first ALE-based assessment method was proposed in which collected kinds of details such as assets, threat, vulnerability etc. to get the expectation of all attacks’ loss. Its disadvantage is that the workload for data collection is so huge. Proposed a method based on BP neural network. a bank, the government and the army etc., its security manager in headquarter needs to monitor the running of all their branches’ networks and takes measures in response when necessary. He also needs to evaluate the network security situation in an area to measure the performance of subordinate network managers. This evaluation model is applicable to some kind of network that is widely spread, has complicated topology, and needs highly security assurance, such as armies, banks, governments, and so on. In detail, this module is based on the assumptions.

The definition of assets here is slightly different from economic s. Assets in the evaluation model are a series of network elements such as software, hardware, data, service, and so on. Software includes operation systems, kinds of applications; hardware includes hosts, servers, routers, fire wall etc. service includes FTP, HTTP and TELNET etc. With the blasting growing of internet, network has been part of people’s life. A network intrusion usually happens based on the following situations: there are vulnerabilities in some software or some service; the password is too simple.

**CHAPTER 3**

**SYSTEM STUDY**

**EXISTING SYSTEM**

Unsupervised outlier detection techniques are playing big role in a various application domains such as network intrusion detection, fault detection and fraud detection. The beauty of unsupervised method is that, it does not require any training data set or any kind of previous knowledge. This technique can help to detect accurate and novel attacks without any previous knowledge the rapid proliferation of the Computer based system and Internet technologies, the most of the problems arises in data privacy, information security and network security has become very prominent. In recent years, cyber-attack and network security incidents show a rising trend. Existing System Detection Delay and cost effective of the process As an intrusion detection system to handle the enormous volume of information, it is also need to update the structure of an effective intrusion detection system is a complex and large process. Depending on the application, constraints on data traffic can be diverse, prioritizing features such as real-time capability, reliability, scalability, deterministic behavior, and low pow er consumption.

|  |  |  |
| --- | --- | --- |
| Reference no. | Technique | Accuracy (%) |
| Zhu [3] | Clustering and Classification | 85.92 |
| Leu [4] | Forensics | 99 |
| Leu [5] | Forensics and Data mining | 94.29 |
| Salunkhe[6] | Machine Learning | 99.33 |
| This paper | Forensics and Neural network | 98.13/99.40/99.42 |

Table.3. 1 Comparison with Existing Literature

# DISADVANTAGES

* Cost Effective of Intrusion Detection
* Attack Detection Slow
* Easily intrusion and transmission delay
* Maintenance difficult

# PROPOSED SYSTEM

Intrusion crimes is increasing day by day. Hence there is need to find the optimal intrusion detection system when compared to the intrusion detection systems that use the traditional Intrusion Detection Efficient Routing Algorithm (IDER). With the network intrusion attacks is becoming more frequent and diverse, the intrusion detection system with a more diverse approach is needed. an intrusion detection system that uses IDER algorithm to detect the type of intrusion and the number of clusters (k) is not fixed beforehand.in the case of large datasets intrusion detection system that uses IDER algorithm shows comparatively higher accuracy when compared to the intrusion detection systems that uses k-means clustering algorithm.

# ADVANTAGES:

* Optimize the quality of routing the data between Source and Destination
* Security is achieved with the help of Routing path
* This performance are reliability of Detection.
* Low Cost of this Detection Process
* Flexible Data Access

# PROPOSED DIAGRAM



**Source**

**Data**

**Data**

**path**

3.2 Detection Efficient Routing Algorithm (ADER)

# CHAPTER 4

**SYSTEM REQUIREMENTS HARDWARE REQUIREMENTS**

CPU type : dual core

Clock speed : 3.0 GHz

RAM size : 2 GB

Hard disk capacity : 250 GB

Monitor type : 15 Inch Color Monitor

Keyboard type : Internet Keyboard

CD -drive type : 52xmax

# SOFTWARE REQUIREMENTS

Operating System : Windows XP

Front End : C # .N E T

Back End : Microsoft Sql server 2005

Documentation : MS- Office

# CYGWIN

Cygwin is the one type of interface tool it is used to interface between source and package and its protocol. Its support the all trace graph and its supported files. It’s mainly used for only visualization purpose.

Some of the program features are as follows:

* 238 2D graphs: Trace graph supports drawing 238 different graphs depending upon different parameters in 2-Dimensional area.
* 12 3D graphs: Trace graph supports 12 graphs in 3 Dimensions.
* Delays, jitter, processing times, round-trip times, throughput graphs and statistics can be plotted with the help of Trace graph. These are described below:
* Delay: This is the delay encountered between the sending and receiving of the packet.
* Jitter: This is the unwanted variation in the output.
* Processing Time: The time it takes for a node to process the input.
* Round Trip Time: The time required for a signal pulse to travel from a specific source to a specific destination and back again.
* Whole network, link and node graphs, and statistics.
* All the results can be saved to text files, graphs can also be saved as jpeg and tiff.
* An y graph saved in the text file with 2 or 3 columns can be plotted.
* Script files processing to do the analysis automatically.
* The program does have some disadvantages though, such as it hangs or takes a very long time while trying to open large trace files. Al so, it sometimes hangs after displaying the graph in 3D. The reason why this tool was used in the simulation work is that there are not too many graph plotting tools available in the market.

# SCENARIO FILE

As CBR file is used to store the traffic connections, similarly scenario file is used to store the initial position of the nodes and movement of nodes at different times and their speed, etc.

Since it will be difficult to manually give initial position, movement of the nodes and their speed for each movement at different times we use a random file generator here also. The node movement generator is available under /indep-

utils/cmu-scen- gen/setdest/ directory. It is available under the name “setdest”, which is an exe file. This file is run with certain arguments to create the scenario file.

The arguments are:

* Number of nodes
* Pause time
* Maximum speed
* Simulation time
* X-axis dimension
* Y-axis dimension

# NETWORK SIMULATOR-2

After setting up the platform, software named ns2 was set up on it which was used for all the analysis and simulation work apart from other tools used. Ns2 is the de facto standard for network simulation. Its behavior is highly trusted within the networking community. It is developed at ISI, California, and is supported by the DARPA and NSF. Ns2 is an object-oriented simulator, written in C++, with an OTcl interpreter as a frontend. This means that most of the simulation scripts are created in Tcl. If the components have to be developed for ns2, then both Tcl and C++ have to be used. Ns2 uses two languages because any network simulator, in general, has two different kinds of things it needs to do. On the one hand, a detailed simulation of protocols requires a systems programming language which can efficiently manipulate bytes, packet headers, and implement algorithms that run over large datasets.

For these tasks run-time speed is important and turn-around time (run simulation, find a bug, fix a bug, recompile, re-run) is less important. On the other hand, a large part of network research involves slightly varying parameters or configurations or quickly exploring a number of scenarios. In these cases, iteration time (change the model and re-run) is more important. Since the configuration runs once (at the beginning of the simulation), the run- time of this part of the task is less important.

# STRUCTURE OF NS-2

* Create the event scheduler
* Turn on tracing
* Create a network
* Setup routing
* Insert errors
* Create a transport connection
* Create traffic
* Transmit application-level data

# NETWORK SIMULATOR 2.28 (NS2)

Ns-2 is a packet-level simulator and essentially a centric discrete event scheduler to schedule the events such as packet and timer expiration. Centric event scheduler cannot accurately emulate "events handled at the same time" in the real world, that is, events are handled one by one. This is not a serious problem in most network simulations, because the events here are often transitory. Beyond the event scheduler, ns-2 implements a variety of network components and protocols.

Notably, the wireless extension, derived from CMU Monarch Project, has 2

assumptions simplifying the physical world:

Nodes do not move significantly over the length of time they transmit or receive a packet. This assumption holds only for mobile nodes of high-rate and low- speed. Consider a node with the sending rate of 10Kbps and moving speed of 10m/s, during its receiving a packet of 1500B, the node moves 12m. Thus, the surrounding can change significantly and cause reception failure. Node velocity is insignificant compared to the speed of light. In particular, none of the provided propagation models include Doppler effects, although they could.

# FUNCTIONALITIES OF NS- ALLIONE 2. 28

C++/OTcl Linkage

Root of ns-2 object hierarchy Bind (): link variable

values between TclObject- C++ and OTcl

Command (): link OTcl methods to C++ implementations TclClass

Create an OTcl object, and create a linkage between the OTcl object and C++Object Tcl C++ - methods to access Tcl interpreter Tcl

command - Standalone global commands EmbeddedTcl -ns script initialization

# HOW TO START TCL SCRIPTS

We can write were Tcl scripts in any text editor like joe or emacs. First of all, we need to create a simulator object. This is done with the command set ns [new Simulator] Now we open a file for writing that is going to be used for the nam trace data. Set nf [open out.nam w] $n s namtrace-all $nf The first line opens the file 'out.nam' for writing and gives it the file handle 'nf'. In the second line, we tell the simulator object that we created above to write all simulation data that is going to be relevant for nam into this file. The next step is to add a 'finish' procedure that closes the trace file and starts nam.

# NETWORK COMPONENTS

The root of the hierarchy is the TclObject class that is the superclass ofall OTcl library objects (scheduler, network components, timers and the other objects including NAM related ones). As an ancestor class of TclObject, N sObject class is the superclass of all basic network component objects that handle packets, which may compose compound network objects such as nodes and links. The basic network components are further divided into two subclasses, Connector, and Classifier, based on the number of the possible output data paths. The basic network objects that have only one output data path are under the Connector class, and switching objects that have possible multiple output data paths are under the Classifier class.

# PACKET

An NS packet is composed of a stack of headers, and an optional data space. A packet header format is initialized when a Simulator object is created, where a stack of all registered (or possibly useable) headers such as the common header that is commonly used by any objects as needed. IP header, TCP header, RTP header (UDP uses RTP header) and trace header, is defined, and the offset of each header in the stack is recorded. What this means is that whether or not a specific header is used, a stack composed of all registered headers is created when a packet is allocated by an agent, and a network object can access any header in the stack of a packet it processes using the corresponding off set value.

# STARTING NAM

NAM is a Tcl/TK based animation tool for viewing network simulation traces and real world packet trace data. The first step to use NA M is to produce the trace file.

The trace file should contain topology information, e.g., nodes, links, as well a s packet traces. Usually, the trace file is generated by ns2. During an ns2 emulation, the user can produce topology configurations, layout information,

and packet traces using tracing events in ns2. When the trace file is generated, it is ready to be animated by NAM. Upon startup, NAM will read the trace file, create the topology, pop up a window, do a layout if necessary and then pause at the time of the first packet in the trace file. Through its user interface, NA M provides control over many aspects of animation.

# TRACE GRAPH

Trace graph is a free tool for analyzing the trace files generated by ns2. Trace graph can support any trace for m at if converted to its own or ns2 trace format. Trace graph run s under Windows, Linux, and UN IX and MAC OS systems. Some of the program features are as follows:

* 238 2D graphs: Trace graph supports drawing 238 different graphs depending upon different parameters in 2 Dimensional areas.
* 12 3D graphs: Trace graph supports 12 graphs in 3 Dimensions.
* Delays, jitter, processing times, round-trip times, throughput graphs and statistics can be plotted with the help of Trace graph. These are described below:
* Delay: This is the delay encountered between the sending and receiving of the packet.
* Jitter: This is the unwanted variation in the output.
* Processing Time: The time it takes for a node to process the input.
* Round Trip Time: The time required for a signal pulse to travel from a specific source to a specific destination and back again.
* Whole network, link and node graphs, and statistics.
* All the results can be saved to text files, graphs can also be saved as jpeg and tiff.
* An y graph saved in the text file with 2 or 3 columns can be plotted.
* Script files processing to do the analysis automatically.

# SCENARIO FILE

As CBR file is used to store the traffic connections, similarly scenario file is used to store the initial position of the nodes and movement of nodes at different times and their speed, etc. Since it will be difficult to manually give initial position, movement of the nodes and their speed for each movement at different times we use a random file generator here also. Number of nodes

* Pause time
* Maximum speed
* Simulation time
* X-axis dimension
* Y-axis dimension

# THE ADVANTAGES OF NETWORKING

Networks allow computers, and hence their users, to be connected together. The y also allow for the easy sharing of information and resources, and cooperation between the devices in other ways. Some of the major benefits are:

# CONNECTIVITY AND COMMUNICATION

Networks connect computers and the users of those computers. Individuals within a building or work group can be connected into LAN.

# DATA SHARING

One of the most important uses of networking is to allow the sharing of data. True networking allows thousands of employees to share data much more easily and quickly.

# HARDWARE SHARING

Networks facilitate the sharing of hardware devices. For example, instead of giving each of 10 employees in a department an expensive color printer, one printer can be placed on the network for everyone to share.

# INTERNET ACCESS

The Internet is itself an enormous network. The significance of the Internet on modern society is hard to exaggerate, especially for technical fields. Internet Access Sharing.

Small computer networks allow multiple users to share a single Internet connection. Special hardware devices allow the bandwidth of the connection to be easily allocated to various individuals as they need it.

# DATA SECURITY AND MANAGEMENT

In a business environment, a network allows the administrators to much better manage the company's critical data.

# LINK

A link is another major compound object in NS. When a user creates a ink using a duplex-link member function of a Simulator object, two simplex linksin both directions are created. One thing to note is that an output queue of a node is actually implemented as a part of a simplex link object. Packets dequeued from a queue are passed to the Delay object that simulates the link delay, and packets dropped at a queue are sent to a Null Agent and are freedthere. Finally, the TTL object calculates Time to live parameters for each packet received and updates the TTL field of the packet.

# STARTING NS

NS starts with the command ns (assuming that we are in the directory with the ns executable, or that were path points to that directory), where is the name of a Tcl script file which defines the simulation scenario We could also just start ns without any arguments and enter the Tcl commands in the Tcl shell, but that is definitely less comfortable. Everything else depends on the Tcl script. The script might create some output, it might write a trace file or it might start nam to visualize the simulation.

* + FEASIBILITY STUDY
  + Technology and system feasibility

The assessment is based on an outline design of system requirements in terms of Input, Processes, Output, Fields, Programs, and Procedures. This can be quantified in term s of volumes of data, trends, frequency of updating, etc. in order to estimate whether the new system will perform adequately or not.

# ECONOMIC FEASIBILITY

Economic analysis is the most frequently used method for evaluating the effectiveness of a new system. M ore commonly known as cost/benefit analysis, the procedure is to determine the benefits and savings that are expected from a candidate system and compare them with costs. An entrepreneur must accurately weigh the cost versus benefits before taking an action.

# COST BASED STUDY

It is important to identify cost and benefit factors, which can be categorized as follows

* Development costs; and
* Operating costs.

This is an analysis of the costs to be incurred in the system and the benefits derivable out of the system.

# TIME BASED STUDY

This is an analysis of the time requ ire d to achie ve a return on investments. The benefits derived from the system. The future value of a project is also a factor. As per the cost based study this system requires the designing and implementing environment as listed below

# LEGAL FEASIBILITY

Determines whether the proposed system conflicts with legal requirements, e.g., a data processing system must comply with the local Data Protection Acts. This system satisfies all the legal requirements and it also complying with the local data protection act.

# OPERATIONAL FEASIBILITY

Is a measure of how well a proposed system solves the problems, and takes advantage of the opportunities identified during scope definition.

# CHAPTER 5 MODULE DISCRIPTION

**SOURCE NODE**

Source-location privacy protection have lower safety periods, source location privacy protection algorithm based on expected phantom source node is proposed. With coordinates of source node and sink node, the algorithm establishes an ellipse and selects a node randomly on the ellipse as expected phantom source node which providing direction for phantom source node.

# ROUTING PATH

Routing is one of the most essential problems in the telecommunications network. As one of the essential characteristic of both mobile wireless and fixed networks. The underwater communication network can realize the centralized command, overall attack and defense, and resource sharing. It plays the great important role in improving the fighting capacity. Wireless sensor networks are typically deployed in harsh environments or unmanned enemy positions in the area, the broadcast nature of wireless communication.

# INTRUSION DETECTION EFFICIENCY ALGORITHM

Common network information security techniques include firewall technology, intrusion detection technology, anti-virus technology, internal and external network isolation technology and email security, among which intrusion detection technology is undoubtedly the last line of defense of network security.

# SECURE COMMUNICATION

The above algorithm decomposes the analytical model of stream transmission time series in wireless networks into statistics with multiple nonlinear components to extract intrusion anomaly features, but the accuracy of detection is not high.

The types and detection principles of wireless network intrusion detection is analyzed, it adopts the information statistical analysis method to detect the network intrusion, constructs the traffic statistical analysis model of the network abnormal intrusion, and establishes the network intrusion signal model by combining the signal fitting method.

# DESTINATION NODES

Destination node does not have sufficient resources commonly to encode and decode. Furthermore, many terminal destination nodes have a limited arithmetic capability and storage capacity. The simulation results show that the improved decoding scheme can effectively reduce the load of decoding in the destination node. The possession of resource in all nodes is not equivalent. Some terminal nodes are not convenient to replace or upgrade. Therefore, additional storage consumption and computational load are not conducive to the survival of node and the healthy operation of the entire network.

# CHAPTER 6 SYSTEM TESTING

**TESTING PRINCIPLES**

Before applying method to design effective test cases, a software engineer must understand the basic principles that guide software testing. Davis (DAV95) suggests a set of testing principles which have been adapted for use in this book.

* Al l tests should be traceable to customer requirements.
* Test should be planned long before testing begins.
* Test pare to principle applets to software testing. Testing should begin “in the small” and progress towards testing “in the page”.
* Exhaustive testing is not possible.

# UNIT TESTING

Unit testing focuses on verification errors on the smallest unit of software design- the module. Using the procedural design description as a guide, important control paths are tested to uncover errors within the boundary of the module.

# INTEGRATION TESTING

Integration testing is a systematic technique for constructing the program structure while conducting test to uncover errors associated with interfacing. The objective is to take unit tested modules and build a program structure thathas been dictated by design.

# WHITE BOX TESTING

White box testing is some time is called glass box testing, is a test case design that uses a control structure of the procedural design to drive the test cases testing methods, the software engine.

* Guarantee that logical decisions are on the true and false sides
* Exercise all logical decisions are on the true and false sides
* Execute all loops at their boundaries and within their operational bounds
* Exercise internal data structure to assure the validity

# ACCEPTANCE TESTING

Finally when the software is completely built, a series of acceptance tests are conducted to enable the client to validate all requirements. The user conducts these tests rather than the system developer, which can range from informal test drive to a planned and systematical executed series of tests. These acceptance tests are conducted over a period of weeks or months, there by uncovering cumulative errors that might degrade the system order time.

# ALPHA TESTING

The customer conducts the alpha test at the developer’s site. The client notes the errors and usage problems and gives report to the developer. Alpha tests are conducted in a control environment.

# BLACK BOX TESTING

Black box testing focuses on the functional requirements of the software.

* + Performance s in data structures or external database access.
  + Performance errors.
  + Initialization and termination errors.
  + Incorrect or missing functions.

# TEST CASES

Once source code has been generated, software must be tested to uncover (and correct) as many errors as possible before delivery to your customer. Your goal is to design a series of test cases that have a high likelihood of fin ding errors. To do so we have techniques provide systematic guidance for designing tests that: (1)

exercise the internal logic of software components, and exercise the input and output domains of the program to uncover errors in program function, behavior, and performance. Resource presented in this section address the following topic categories. Software Testing is the process of confirming the functionality and correctness of software by running it. Software testing is usually performed for one of two reasons:

* Defect detection
* Reliability estimation.

The problem of applying software testing to defect detection is that software can only suggest the presence of flaws, not their absence (unless the testing is exhaustive). The problem of applying software testing to reliability estimation is that the input distribution used for selecting test cases may be flawed. In both of these cases, the mechanism used to determine whether program output is correct is often impossible to develop.

# SYSTEM IMPLEMENTATION

Implementation includes all those activities that take place to convert from the old system to the new. The new system may be totally new, replacing an existing system or it may be major modification to the system currently put into use.

This system “Access Point Selection for Improving the Voice Quality and Overall Throughput in Wireless LAN s” is a new system.

The System implementation phase consists of the following steps:

* Testing the developed software with sample data.
* Correction of any errors if identified.
* Creating the files of the system with actual data.
* Making necessary changes to the system to find out errors.
* Training of user personnel.

The system has been tested with sample data, changes are made to the user

requirements and run in parallel with the existing system to find out the discrepancies. The user has also been appraised how to run the system during the training period.

This phase is primarily concerned with user training, site preparation and file conversions. During the final testing, user acceptance is tested, followed by user training. Depending in the nature of the extensive user training may be required. However, broad organizational representation, accomplished through the project team, is require d to complete the system development cycle. NET Framework has offer very efficient yet simple implementation techniques for development of the project.

# IMPLEMENTATION PLAN

Implementation is the stage, which is crucial in the life cycle of the new system designed. Implementation means converting a new or revised system design into an operational one. This is the stage of the project where the theoretical design is turned into a working system. In this project “Access Point Selection” implementation includes all those activities that take place to convert from the old system to the new one.

The important phase of implementation plan is change over. The implementation phase’s construction, installation and operations lie on the new system. The most crucial and very important stage in achieving a new successful system and in giving confidence on the new system for the user that it will work efficiently and effectively.

* There are several activities involved while implementing a project:
* Careful planning
* Investigation current system and its constraints on implementation
* Design of methods to achieve the change over
* Training of the staff in the changeover procedure and evaluation of change over method

The implementation is the final stage and it is an important phase. It involves the individual programming system testing, user training and the operational running of developed proposed system that constitutes the application subsystems. The implementation phase of software development is concerned with translating design specifications into source code. The user tests the developed system and changes are made according to their needs.

# CHANGE OVER

The implementation is to be done step by step since testing with dummy data will not always reveal the faults. The system will be subjected to the employees to work. If such error or failure is found, the system can be corrected before it is implemented in full stretch. The trail should be done as long as the system is made sure to function without any failure or errors.

# EDUCATION AND USER TRAINING

Well-designed and technically elegant systems can succeed or fail because of the way they are operated and used. Therefore the quality of the training receive d by the personnel involved with the systems help or hinder, and may even prevent, the successful completion of the system.

An analysis of user training focuses on user capabilities and the nature of the system being installed. Those users are verifying type and nature. The requirements of the system also range from simple to complex tasks. So the training has to be generated to the specific user based on his/her capabilities and system ’s complexity.

# CHAPTER 7

**CONCLUSION**

Most sensitive field of security that is emerging with its immediate needs is database security. Propose an energy efficient routing method in an environment where both Attack detection and prevention schemes are used in WS Ns. Security is one of the most important properties of wireless sensor networks, which are threatened by varied attacks, to approach practical deployment. Database security concerns the use of a broad range of information security controls to protect databases against compromises of their confidentiality, integrity and availability. The data that is taken as part of personal privacy theft is sold in black markets. Hence there is a need to develop an effective and efficient network intrusion detection system for detecting the type of attacks.

# FUTURE ENHANCEMENT

Aims at selecting the optimal transmission route and guaranteeing the effective and reliable Deep Packet Inspection techniques can help to classify flows, but are currently implemented in electronic hardware, which imposes limitations in terms of speed the algorithm Multi-hop transmission link constructed by wireless relay nodes is a feasible solution to long range. Security is an important issue for routing in WSNs, because many applications will affect life-or-death decisions and prohibited tampering can have devastating consequences.

# REFERENCES

1. Hyung-Sin Kim, Jin-Seok Han and Yong-Hwan Lee " Scalable Network JoiningMechanism in Wireless Sensor Networks" IEEE 2012 Page No [45-48]
2. Achim Berger, Albert Potsch and Andreas Springer "Real-Time Data Collection in a Spatially Extended TDMA-based Wireless Sensor Network" IEEE 2012 Page No [41-44]
3. Yuki Nishika wa, Takuya Sasamura, Yoichi Ishizuka, Satoshi Sugimoto, Shohei Iwa saki1, Hongyan Wang, Tomoyuki Fujishim a, Takafumi Fujimoto, K oichiro Yama shita, Takahisa Suzuki, Koji Kurihara "Design of Stable Wireless Sensor Network for Slope Monitoring " IEEE 2018 Page No [8-11]
4. Kyosuke Fukuda, Osamu Takyu, Keiichiro Shirai, Mai Ohta , Takeo Fujii,Fumihito Sasamori, Shiro Handa "Transmit Control and Data Separation in Physical WirelessParameter Conversion Sensor Networks with Event Driven Sensors"IEEE 2018 Page No[12-14]
5. M. Udin Harun Al Rasyid, Ferry Astika Saputra, MH. Ramdhani Ismar "Performance of Multi-hop Networks Using Beacon and Non- beacon Scheduling in Wireless Sensor Network (WSN) “IEEE 2015 Page No [195-199]
6. Manoj Kumar, Robin Mathur "Unsupervised Outlier Detection Technique for Intrusion Detection in Cloud Computing"IEEE 2014 Page No [1-4]
7. Wael Ali Hussein, Borhanuddin M Ali, MFA Rasid, Fazirulhisyam Hashim "Design and Performance Analysis of High Reliability-optimal Routing protocol for Mobile Wireless Multimedia Sensor Networks" IEEE 2015 Page No [136-140]
8. Mithun Mukherjee ; Lei Shu ; Wei Fang ; Zhangbing Zhou " Sleep Scheduling in Wireless Powered Industrial Wireless Sensor Networks" IEEE 2017 Page No

[301- 302]

1. AbelRodriguez dela Concepcion, Riccardo Stefanelli, Daniele Trinchero "Adaptive Wireless Sensor Networks for High-Definition Monitoring in Sustainable Agriculture " IEEE 2014 Page No [67-69]

# SOURCE CODE

set val(chan) Channel/WirelessChannel ;# channel type

set val(prop) Propagation/TwoRayGround ;# radio-propagation modelsetval(netif) Phy/WirelessPhy ;# network interface type set val(mac) Mac/802\_11 ;# MAC type

set val(ifq) Queue/DropTail/PriQueue ;# interface queue typesetval(ll)LL ;# link layer type

set val(ant) Antenna/OmniAntenna ;# antenna modelset val(ifqlen) 50 ;# max packet in ifq

|  |  |  |
| --- | --- | --- |
| set val(nn) | 22 | ;# number of mobilenodesset |
| val(rp) | SDTRP | ;# routing protocol |
| set val(x) | 4546 | ;# X dimension of topography |
| set val(y) | 1000 | ;# Y dimension of topography |
| set  val(stop) | 7.0 | ;# time of simulation end |

#Create a ns simulator set ns [new Simulator] #Setup topography object

set topo [new Topography]

$topo load\_flatgrid $val(x)

$val(y)create-god $val(nn)

#Open the NS trace file set tracefile [open out.tr w]

$ns trace-all $tracefile #Open the NAM trace file set namfile [open out.nam w]

$ns namtrace-all $namfile

$ns namtrace-all-wireless $namfile $val(x) $val(y) set chan[new $val(chan)];#Create wireless channel

$ns node-config -llType $val(ll) \

-macType $val(mac) \

-ifqType $val(ifq) \

-ifqLen $val(ifqlen) \

-antType $val(ant) \

-propType $val(prop) \

-phyType $val(netif) \

-adhocRouting AODV \

-channel $chan \

-topoInstance $topo \

-agentTrace ON \

-routerTrace ON \

-macTrace ON \

-movementTrace ON

$ns color 0 darkgreen

#Create 22 nodessetn0[$ns node]

$n0 set X\_ 109

$n0 set Y\_ 174

$n0 set Z\_ 0.0

$ns initial\_node\_pos $n0 30setn1 [$ns node]

$n1 set X\_ 79

$n1 set Y\_ 86

$n1 set Z\_ 0.0

$ns initial\_node\_pos $n1 30setn2 [$ns node]

$n2 set X\_ 397

$n2 set Y\_ 528

$n2 set Z\_ 0.0

$ns initial\_node\_pos $n2 30setn3 [$ns node]

$n3 set X\_ 557

$n3 set Y\_ 583

$n3 set Z\_ 0.0

$ns initial\_node\_pos $n3 30set

$n4 set Y\_ 766

$n4 set Z\_ 0.0

$ns initial\_node\_pos $n4 30setn5 [$ns node]

$n5 set X\_ 757

$n5 set Y\_ 713

$n5 set Z\_ 0.0

$ns initial\_node\_pos $n5 30setn6 [$ns node]

$n6 set X\_ 542

$n6 set Y\_ 816

$n6 set Z\_ 0.0

$ns initial\_node\_pos $n6 30setn7 [$ns node]

$n7 set X\_ 314

$n7 set Y\_ 138

$n7 set Z\_ 0.0

$ns initial\_node\_pos $n7 30setn8 [$ns node]

$n8 set X\_ 519

$n8 set Y\_ 211

$n8 set Z\_ 0.0 set n9 [$ns node]

$n9 set X\_ 757

$n9 set Y\_ 203

$n9 set Z\_ 0.0

$ns initial\_node\_pos $n9 30setn10 [$ns node]

$n10 set X\_ 822

$n10 set Y\_ 418

$n10 set Z\_ 0.0

$ns initial\_node\_pos $n10 30setn11 [$ns node]

$n11 set X\_ 949

$n11 set Y\_ 620

$n11 set Z\_ 0.0

$ns initial\_node\_pos $n11 30setn12 [$ns node]

$n12 set X\_ 1057

$n12 set Y\_ 375

$n12 set Z\_ 0.0

$ns initial\_node\_pos $n12 30setn13 [$ns node]

$n13 set X\_ 1279

$n13 set Z\_ 0.0

$ns initial\_node\_pos $n13 30setn14

[$ns node]

$n14 set X\_ 1164

$n14 set Y\_ 603

$n14 set Z\_ 0.0

$ns initial\_node\_pos $n14 30setn15 [$ns node]

$n15 set X\_ 1064

$n15 set Y\_ 141

$n15 set Z\_ 0.0

$ns initial\_node\_pos $n15 30setn16 [$ns node]

$n16 set X\_ 912

$n16 set Y\_ 48

$n16 set Z\_ 0.0

$ns initial\_node\_pos $n16 30setn17 [$ns node]

$n17 set X\_ 1272

$n17 set Y\_ 93

$n17 set Z\_ 0.0

$n18 set X\_ 1334

$n18 set Y\_ 228

$n18 set Z\_ 0.0

$ns initial\_node\_pos $n18 30setn19

[$ns node]

$n19 set X\_ 109

$n19 set Y\_ 621

$n19 set Z\_ 0.0

$ns initial\_node\_pos $n19 30setn20 [$ns node]

$n20 set X\_ 509

$n20 set Y\_ 400

$n 20 set Z\_ 0.0

$ns initial\_node\_pos $n20 30setn21 [$ns node]

$n21 set X\_ 752

$n21 set Y\_ 1205

$n 21 set Z\_ 0.0

$ns initial\_node\_pos $n21 30setn22 [$ns node]

$n22 set X\_ 643

$n22 set Y\_ 1005

$ns initial\_node\_pos $n22 30setn23 [$ns node]

$n23 set X\_ 543

$n23 set Y\_ 1105

$n 23 set Z\_ 0.0

$ns initial\_node\_pos $n23 30setn24 [$ns node]

$n24 set X\_ 432

$n24 set Y\_ 1305

$n 24 set Z\_ 0.0

$ns initial\_node\_pos $n24 30setn25 [$ns node]

$n25 set X\_ 353

$n25 set Y\_ 425

$n 25 set Z\_ 0.0

$ns initial\_node\_pos $n25 30setn26 [$ns node]

$n26 set X\_ 207

$n26 set Y\_ 985

$n 26 set Z\_ 0.0

$ns initial\_node\_pos $n26 30

}

node Id = amac\_M AX\_N U M \_ N EIG HBORS; schedId

= amac\_MAX\_NUM\_SCHEDULES;

for (i = 0; i < vechile; i++) {

if (neighbList\_[i].state > 0 && neighbList\_[i].nodeId == sf->sr c Addr) { nodeId = i;

schedId = neighbList\_[i].schedId;

}

}

}

#Define a 'finish' procedureproc finish {} {

global ns tracefile namfile

$ns flush-trace close

$tracefile close

$namfile

exec ./xgraph throughput.tr deliveryratio.tr packetdelay.tr -t "Proposed S ystem " -x "Time "

-y " N o. of Packet" -bg white &

exec ./xgraph e-throughput.tr e-deliveryratio.tr e-packetdelay.tr -t "Existing System " -x "Time"

-y " N o. of Packet" -bg white & exec

./nam out.nam & exit 0

}

for {set i 0} {$i < $val(nn) } { incr i } {

$ns at $val(stop) "\$n$i reset"

}

$ns at $val(stop) "$ns nam-end-wireless $val(stop)"

$ns at $val(stop) "finish"

$ns at $val(stop) "puts \"done\" ; $ns halt"

$ns run